identify the means by which destruction will occur, i.e., shredding, burning, electronic erasure, etc.

(12) *Comptroller General access*. Include a statement that the Comptroller General may have access to all records of the recipient agency to monitor or verify compliance with the terms of the CMA.

(13) *Cost-benefit analysis*. (i) A cost-benefit analysis shall be conducted for the proposed computer matching program unless:

(A) The Data Integrity Board waives the requirement, or

(B) The matching program is required by a specific statute.

(ii) The analysis must demonstrate that the program is likely to be cost-effective. This analysis is to ensure agencies are following sound management practices. The analysis provides an opportunity to examine the programs and to reject those that will only produce marginal results.

APPENDIX A TO PART 310—SAFEGUARDING PERSONALLY IDENTIFIABLE INFORMATION (PII)

(See §310.13 of Subpart B)

A. GENERAL

1. The IT environment subjects personal information to special hazards as to unauthorized compromise, alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in IT systems consistent with the requirements of DoD Directive 8500.1 and DoD Instruction 8500.2.

2. Personally identifiable information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. IT facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated "For Official Use Only." (See DoD 5200.1–R.)

B. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse. (See OMB Circular A–130 and DoD Instruction 8500.2.)

2. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. MINIMUM ADMINISTRATIVE SAFEGUARDS

The minimum safeguarding standards as set forth in §310.13(b) apply to all personal data within any IT system. In addition:

1. Consider the following when establishing IT safeguards:

a. The sensitivity of the data being processed, stored and accessed.

b. The installation environment.

c. The risk of exposure.

d. The cost of the safeguard under consideration.

2. Label or designate media products containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products "For Official Use Only" in accordance with the requirements of DoD 5200.1–R satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with the requirements of DoD 5200.1–R and DoD Directive 8500.1.

4. Mark and protect all computer products containing "For Official Use Only" material in accordance with the requirements of DoD 5200.1–R.

5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

7. Train personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

D. PHYSICAL SAFEGUARDS

1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

3. Safeguard on-line devices directly coupled to IT systems that contain or process information from systems of records to prevent unauthorized disclosure, use, or alteration.

4. Dispose of paper records following appropriate record destruction procedures. (See §310.13(c) and DoD 5200.1–R.)

E. TECHNICAL SAFEGUARDS

1. Components are to ensure that all PII not explicitly cleared for public release is protected according to Confidentially Level Sensitive, as established in DoD Instruction 8500.2. In addition, all DoD information and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing.

2. Encrypt unclassified personal information in accordance with current Information Assurance (IA) policies and procedures, as issued.

3. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

4. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

5. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to IA controls specified in DoD Instruction 8500.2.

6. Remote access for processing PII should comply with the latest IA policies and procedures.

7. Minimize access to data fields necessary to accomplish an employee's task-normally, access shall be granted only to those data elements (fields) required for the employee to perform his or her job rather than granting access to the entire database.

8. Do not totally rely on proprietary software products to protect personnel data during processing or storage.

F. SPECIAL PROCEDURES

1. Managers shall:

a. Prepare and submit for publication all system notices and amendments and alterations thereto. (See §310.30(f).)

b. Identify required controls and individuals authorized access to PII and maintain updates to the access authorizations.

c. When required, ensure Privacy Impact Assessments are prepared consistent with the requirements of the DoD Deputy Chief Information Officer Memorandum, "DoD Privacy Impact Assessment Guidance," October 28, 2005.

d. Train all personnel whose official duties require access to the system of records in the proper safeguarding and use of the information and ensure that they receive Privacy Act training.

G. RECORD DISPOSAL

1. Dispose of records subject to this Regulation so as to prevent compromise. (See §310.13(c).) Magnetic tapes or other magnetic medium may be cleared by degaussing, overwriting, or erasing. (See DoD Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001.)

2. Do not use respliced waste computer products containing personal data.

APPENDIX B TO PART 310—SAMPLE NOTIFICATION LETTER

(See §310.14 of subpart C)

Dear Mr. John Miller:

On January 1, 2006, a Department of Defense (DoD) laptop computer was stolen from the parked car of a DoD employee in Washington, DC after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission at its Web site at *http://www.consumer.gov/idtheft/con_steps.htm*. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The DoD takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.